Figure 1: Network Architecture Diagram
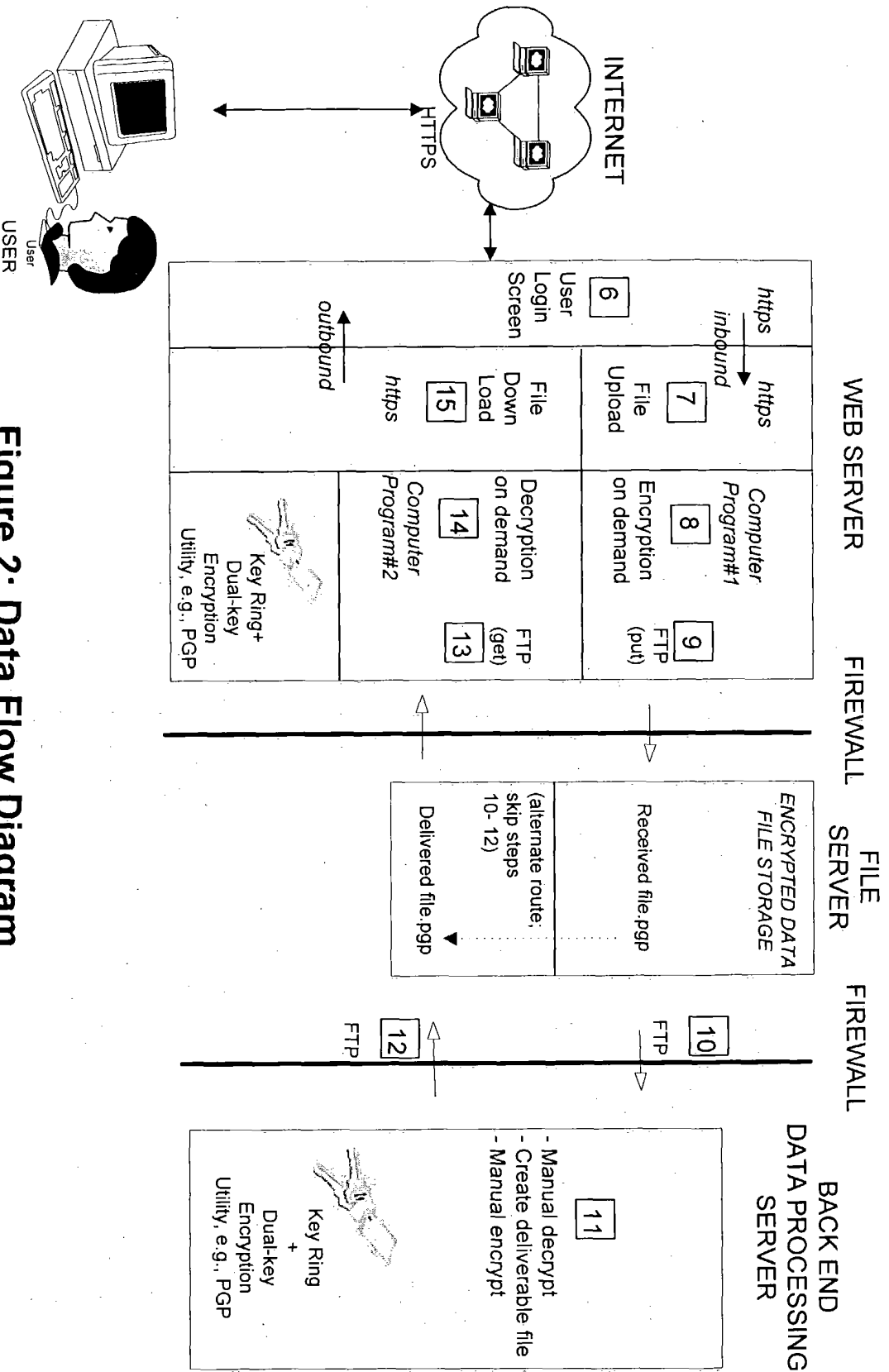
Figure 2: Data Flow Diagram

INTERNET

HTTPS

USER
User

WEB SERVER

https
inbound

https
outbound

User
Login
Screen

6

File
Upload

7

File
Down
Load

https

15

Computer
Program#1

8

Encryption
on demand

9
FTP
(put)

Computer
Program#2

14
Decryption
on demand

13
FTP
(get)

Key Ring+
Dual-key
Encryption
Utility, e.g., PGP

FIREWALL

FILE
SERVER

ENCRYPTED DATA
FILE STORAGE

Received file.pgp

(alternate route;
skip steps
10-12)

Delivered file.pgp

10
FTP

12
FTP

FIREWALL

BACK END
DATA PROCESSING
SERVER

11
- Manual decrypt
- Create deliverable file
- Manual encrypt

Key Ring
+
Dual-key
Encryption
Utility, e.g., PGP

ENCRYPTION-ON-
DEMAND
Computer Program #1

DECRYPTION-ON-
DEMAND
Computer Program #2

START

START

16 | Read Unencrypted Text in RAM

19 | Read Encrypted Text from File into RAM

17 | Encrypt Text in RAM (via PGP call)

20 | Decrypt the Encrypted Text in RAM (via PGP call) and Delete the File Containing the Encrypted Text
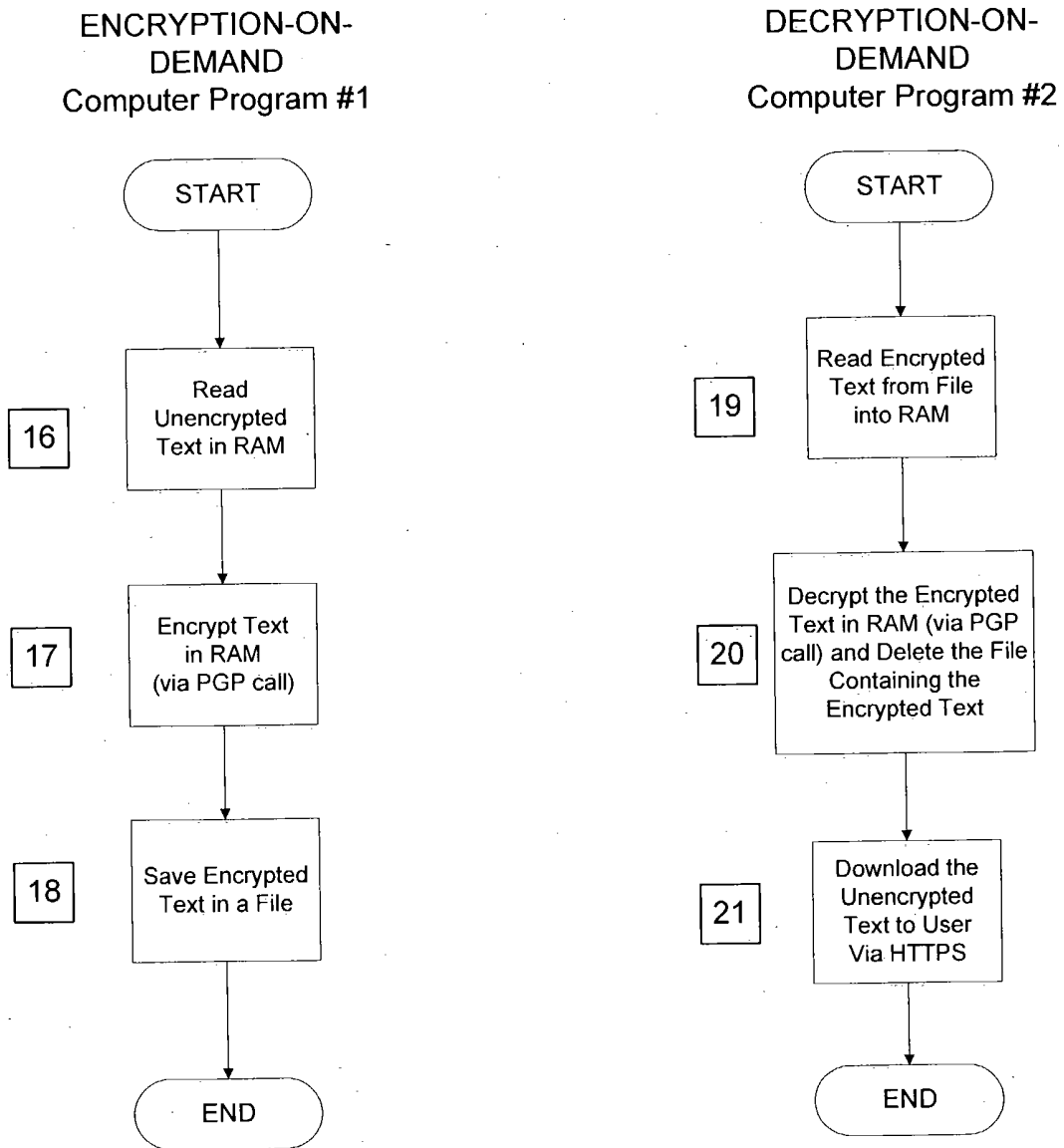
18 | Save Encrypted Text in a File

21 | Download the Unencrypted Text to User Via HTTPS

END

END

Figure 3: Program Logic Diagram